Journal of Network and Computer Applications 68 (2016) 65–79

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks

Yunhe Cui [a], Lianshan Yan [a,*], Saifei Li [a], Huanlai Xing [a,*], Wei Pan [a], Jian Zhu [b], Xiaoyang Zheng [b]

[a] *School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China*
[b] *Centec Networks, Suzhou, China*

ARTICLE INFO

Article history:
Received 21 July 2015
Received in revised form
1 February 2016
Accepted 6 April 2016
Available online 7 April 2016

Keywords:
Software Defined Network (SDN)
Distributed Denial of Service (DDoS)
OpenFlow
Security
Detection
Traceback

ABSTRACT

In order to overcome Distributed Denial of Service (DDoS) in Software Defined Networking (SDN), this paper proposes a mechanism consisting of four modules, namely attack detection trigger, attack detection, attack traceback and attack mitigation. The trigger of attack detection mechanism is introduced for the first time to respond more quickly against DDoS attack and reduce the workload of controllers and switches. In the meantime, the DDoS attack detection method based on neural network is implemented to detect attack. Furthermore, an attack traceback method taking advantages of the characteristics of SDN is also proposed. Meanwhile, a DDoS mitigation mechanism including attack blocking and flow table cleaning is presented. The proposed mechanism is evaluated on SDN testbed. Experimental results show that the proposed mechanism can quickly initiate the attack detection with less than one second and accurately trace the attack source. More importantly, it can block the attack in source and release the occupied resources of switches.

1. Introduction

Software-defined-networking (SDN) offers flexible network management by decoupling forwarding and control planes Software-defined networking. In the SDN architecture, network management is logically centralized at the control plane, while the forwarding plane only needs to forward packets under the manipulation of the control plane. Due to its flexibility, programmability and maintainability, SDN has been widely studied for its applications in backbone networks, data centers, enterprise networks, access networks, wireless networks, and etc. (Jain et al., 2013; Luo et al., 2012; Wang et al., 2016). As an emerging architecture, SDN is facing with security issues that seem to be quite an obstacle to overcome (Collings and Liu, 2014; Sezer et al., 2013; Shin and Gu, 2013; Yan and Yu, 2015). So far, seven main potential security issues have been presented in Kreutz et al. (2013), including forged or faked traffic flows, attacks on vulnerabilities in switches, attacks on control plane communications, attacks on the vulnerabilities in controllers, lack of mechanisms to guarantee trust between the controller and management applications, attacks on vulnerabilities in administrative station and lack of trusted resources for forensics and remediation. However, using easily network programing, network monitoring and dynamic flow policies implementation provided by SDN, network forensics, security policy alteration and security service insertion can be achieved in SDN (Sezer et al., 2013). Among the current security problems, one of the most urgent and hardest security issues is Distributed Denial of Service (DDoS) (Mirkovic and Reiher, 2014). DDoS can easily cause serious damage because it is easy to start, hard to defend and trace. For example, a DDoS attack against Spamhaus has caused huge network congestion in Europe in March 2013 (Answers about recent ddos attack on spamhaus, 2013). Therefore, effectively detecting and resisting DDoS attack in SDN are crucial for future network architecture deployments in SDN.

So far, a number of mechanisms including DDoS attack detection (Braga et al., 2010; Giotis et al., 2014; Mehdi et al., 2011; Miao et al., 2014; Shin et al., 2013; Peng Xiao et al., 2015; Wang et al., 2015; Li et al., 2014), DDoS attack traceback (Francois and Festor, 2015; Zhang et al., 2015) and DDoS attack mitigation (Giotis et al., 2014; Miao et al., 2014; Shin et al., 2013; Wang et al., 2015; Kampanakis et al., 2014) in SDN have already been proposed. Previous studies mainly focus on the detection methods and the mitigation mechanisms. At current, most of the existing detection methods start periodically. However, choosing the proper period of detection loop is hard. If the selected period is too large, the response time (from launching an attack to starting attack detection) will be long, which makes the controller and the switches handle an extremely large

* Corresponding authors.
E-mail address: lsyan@home.swjtu.edu.cn (L. Yan).

http://dx.doi.org/10.1016/j.jnca.2016.04.005
1084-8045/© 2016 Elsevier Ltd. All rights reserved.

amount of attack packets and even destroys the controller and the switches. In contrast, if the period is too small, the attack detection will start more frequently, which makes the controller waste a lot of resources(i.e. CPU and the network bandwidth) and affect the efficiency of the controller. However, as an important factor that affects the detection efficiency and the system performance, the trigger mechanism for detection has not yet attracted much attentions from both academia and industry. Meanwhile, the traceback and mitigation of DDoS attack methods can also be improved to fully use the characteristics of SDN, which may be more valuable for the network security.

In order to solve the problems above, we propose a novel mechanism for resisting DDoS attack in SDN. The mechanism is called Software Defined Anti-DDoS (SD-Anti-DDoS), which is composed of four major modules: Detection Trigger Module, Detection Module, Traceback Module and Mitigation Module. The contribution of the paper is summarized below:

- A SD-Anti-DDoS mechanism is proposed, which consists of DDoS attack detection trigger, DDoS attack detection, DDoS traceback and DDoS attack mitigation in SDN.
- The DDoS attack detection trigger method is presented for the first time to achieve the rapid response of detection module and cope with the limitations of the fixed detection loop approach.
- A DDoS traceback method is put forward to find out the attack path where the attack traffic passed by using the characteristics of SDN (the ability of querying the total topology and the information of each switch).
- A DDoS mitigation mechanism is proposed for attack blocking and flow table cleaning.

The paper is organized as follows. Sections 2 and 3 describe the background and related works in detail respectively. Then the proposed mechanism is illustrated in Section 4. Experimental results are presented in Section 5 followed by the conclusions in Section 6.

2. Background

2.1. SDN

As shown in Fig. 1, SDN is composed of three layers and two interfaces, including Infrastructure Layer, Control Layer, Application Layer, Southbound Interface and Northbound Interface. The main difference between the traditional Internet architecture and SDN is that the latter decouples the control and forwarding planes (Software-defined networking). In SDN, the control function is decoupled from forwarding and centralized in the software-based SDN controllers. The infrastructures only need to accept the instructions from controllers and forward the coming packets under the instructions. It is easy to configure, manage, maintain and protect the entire network for managers through intelligent orchestration systems by decoupling the network control function and forwarding.

OpenFlow is the first communication protocol for connecting the control layer and infrastructure layer in SDN (McKeown et al., 2008; The openflow specification version 1.0.0). Now OpenFlow protocol has already become the de-facto standard in SDN. So far six versions of OpenFlow (from version 1.0 to 1.5) have been released. Among them, version 1.0 and version 1.3 are widely used in OpenFlow-enabled switches. In this paper the OpenFlow v1.0 is chosen as the communication protocol for connecting the controller and switches. Slight performance difference may exist between different versions of OpenFlow.

A switch supporting OpenFlow v1.0 consists of a flow table which performs packet lookup and forwarding and a secure channel used to connect the switch to the controller. The flow table is composed of a set of flow entries. Each flow entry contains header fields, counters and actions. Header fields are used to match against the incoming traffic packets. Counters are applied to count packets matched by a certain flow entry and the actions define related actions that will be applied to the matching packets. Fig. 2 shows the architecture of a flow entry. Header fields can be composed of some or all of the following items: ingress port, Ethernet source address, Ethernet destination address, Ethernet type, VLAN id, VLAN priority, IP source address, IP destination address, IP protocol, IP ToS bits, transport source port and transport destination port. Each item of the header fields may have a special value or ANY (a wildcard used to match all value). All items in the header fields will be used to compare with the relevant information of the coming packet. When a new packet arrives through the switch's port, it will be compared with all flow entries' header fields of the flow table one by one until the matched flow entry is found or all flow entries have been compared. Once the relevant fields of the packet match a flow entry, the counters of this flow entry will be updated and the associated actions will be executed. If the packet does not match all existing flow entries in the flow table, the relevant information of that packet will be sent to the controller.

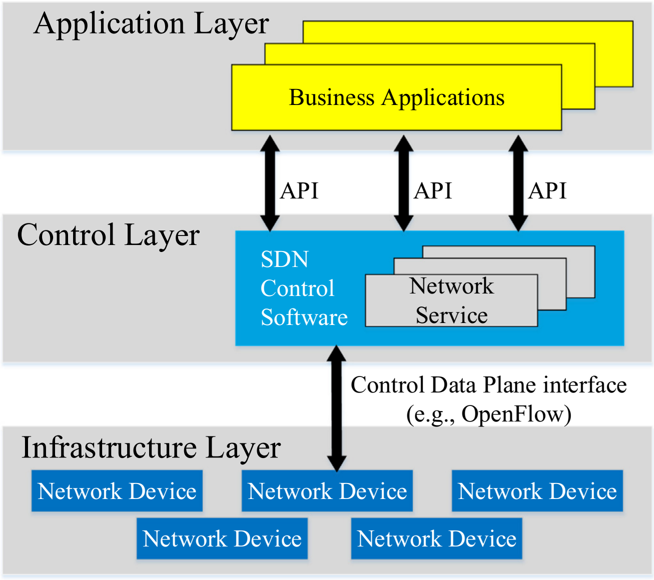

Fig. 1. The architecture of SDN.

2.2. DDoS in SDN

As discussed above, taking advantages of centralized controlling, high programmability and improved automation of SDN, technologies including real-time monitoring, accurate analyzing and rapid response will be supported in SDN. More specifically, SDN can bring the following benefits to DDoS attack protection:

- *Flexible monitoring mechanism:* SDN has ability to implement different kinds of monitoring mechanism. Such as traffic statistics and monitoring about ports or switches, traffic mirroring of special traffic, flow rate monitoring of special traffic and so on. In a word, it is possible to detect DDoS attack using different detection mechanisms by using the flexible monitoring mechanism.
- *Software based detection mechanism:* SDN provides a common programming environment for network managers to control